Open, Programmable, Secure 5G (OPS-5G) Program

Jonathan M. Smith
DARPA Information Innovation Office

Proposers Day
Arlington, VA

January 7, 2020

Goal

Create open source software and systems enabling secure 5G and subsequent mobile networks

From 4G to 5G:

5G Benefits:
10-100x bandwidth
1000x capacity
0.1x latency
100x connections
10x device battery life
Programmability:
- have it your way

OPS-5G

Open Source:
- Increased code visibility
- Hardware/Software decoupling

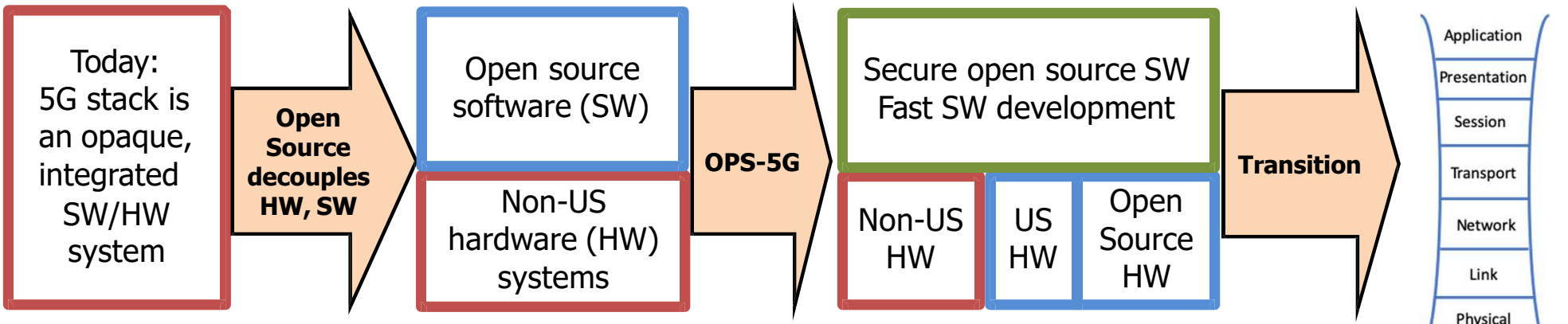
Programmable:
- Bespoke networks
- Adaptation velocity

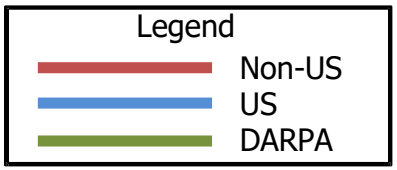
Secure:
- Increase trust at softest points
- Increase defender velocity

5G Risks:
Many untrusted devices
Opaque proprietary software
Non-US hardware
Misuse of programmability
viz Javascript on WWW

Vision: Open, Programmable, Secure 5G (OPS-5G)

OPS-5G will develop a portable standards-compliant network stack for 5G mobile that is free, open source, and *secure by design*



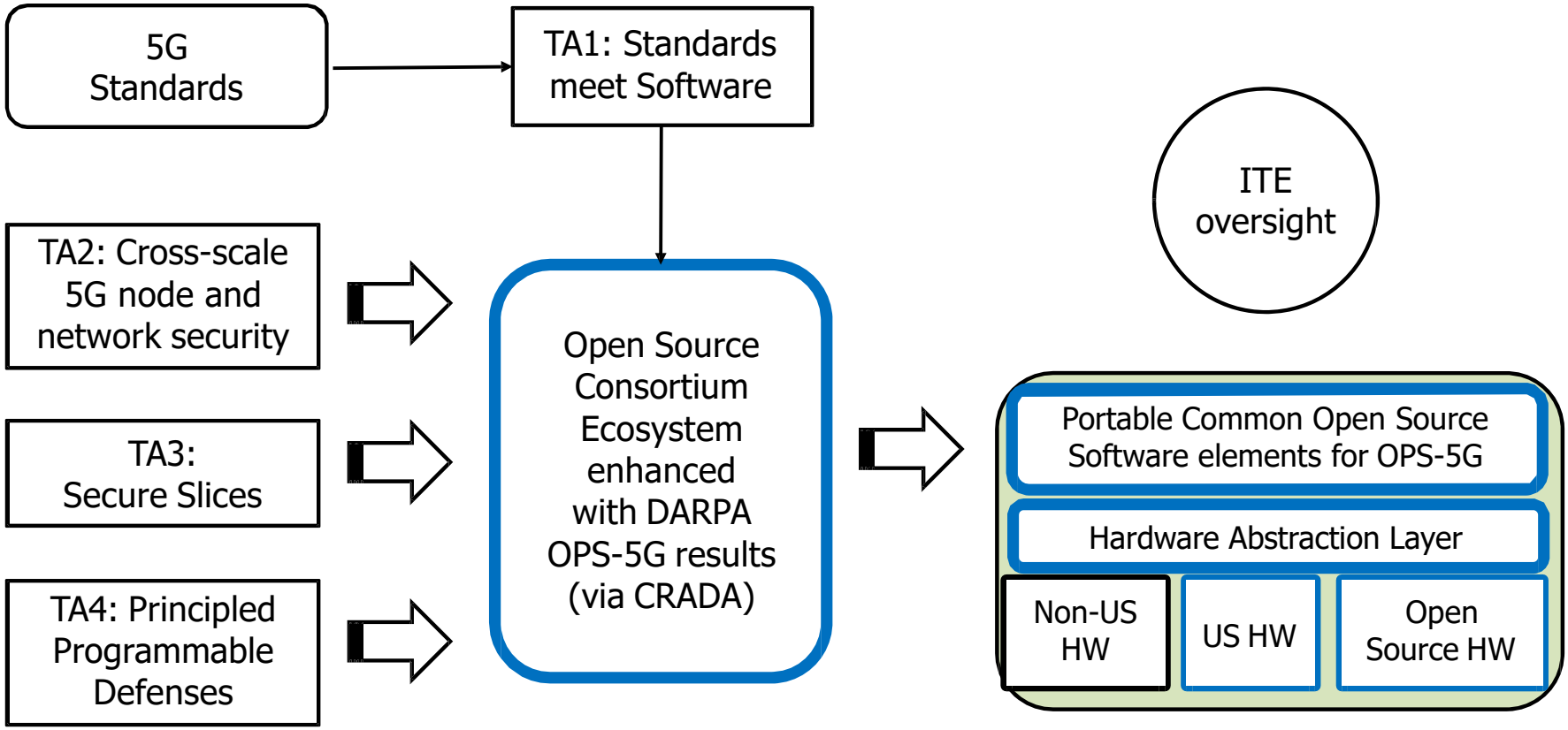


What's New in OPS-5G?

Today	No OPS-5G?	OPS-5G Benefit / TA
Vendor proprietary software	Open source lags in code velocity	Machine Translation adds code velocity TA1: Standards Meet Software
5G-attached Internet of Things (IoT)	Cost pressures elide security	Scalable cost-effective architectural solutions TA2: Many-scale 5G node and network security
Suspect shared resources	Vulnerable to, e.g., side channel leaks	Trusted nets on untrusted infrastructure TA3: Secure slices
5G features open new attacks	Adversary control / denial / agility	Quick and flexible response TA4: Principled programmable defenses

OPS-5G overcomes unmet 5G security needs

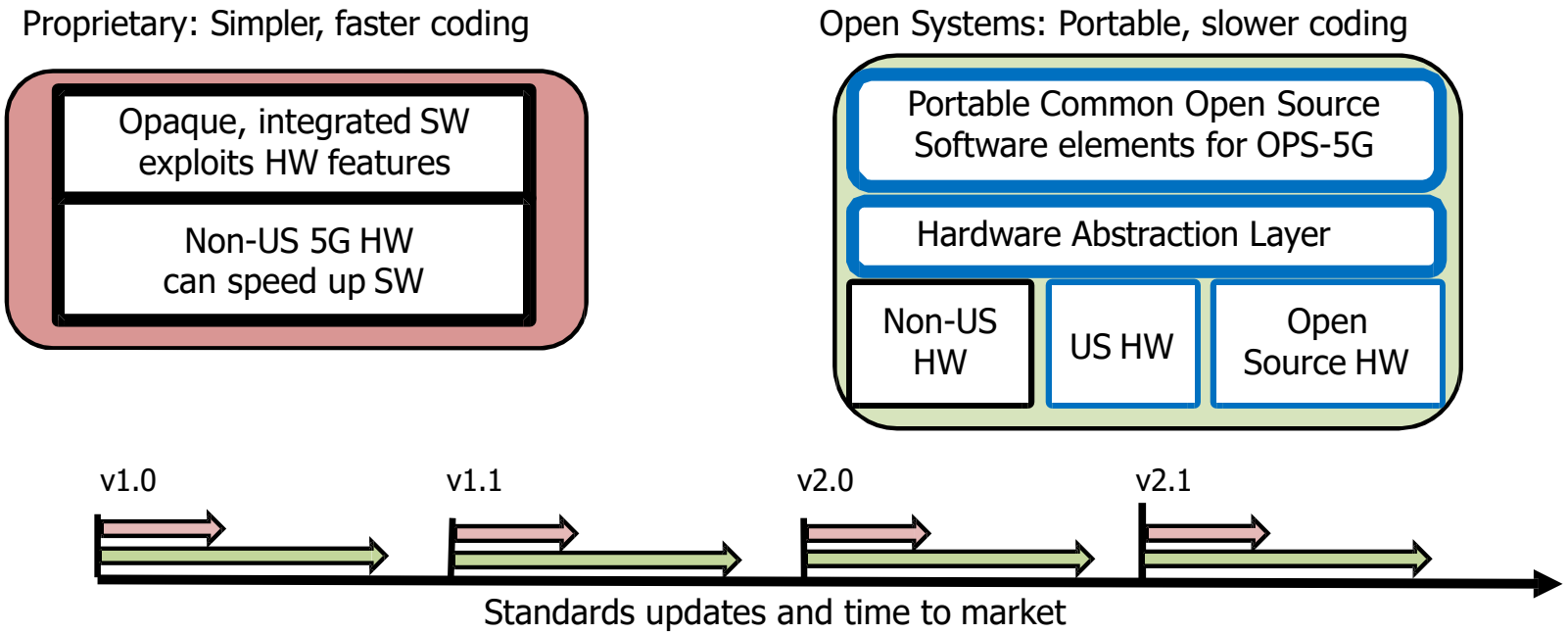
Program Structure and Transition Plan



TA1 Challenge: Hardware/Software Decoupling is Hard!

Issues:

- Requires collaboratively developed, well-defined standards (IETF, etc.)
- Portability requirement increases development complexity and time
- Increased development time exacerbated by evolving standards

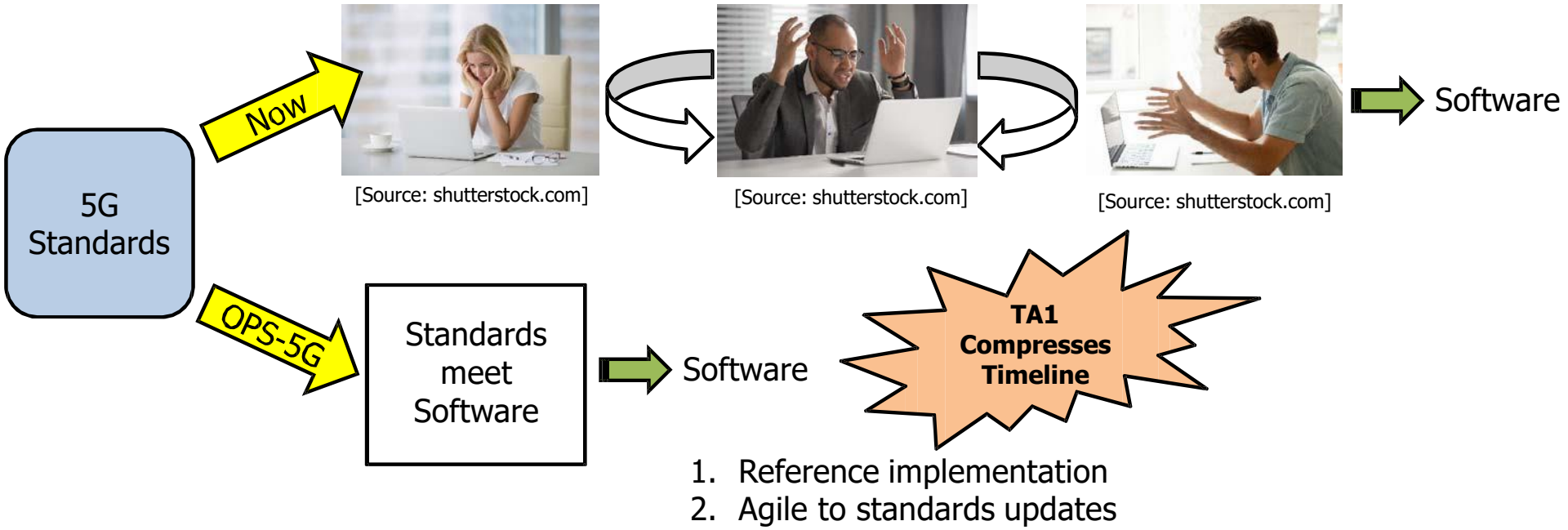


Technical Area 1 – Standards meet Software

Goal: Accelerate development of open source software from standards

Approach: Extend NLP to generate formal machine-readable representation of standards

- Rigid document structure, limited domain in 5G standards enable automated translations
- Promising pathfinders (KANT, ARSENAL, TAILCM)



1. Reference implementation
2. Agile to standards updates

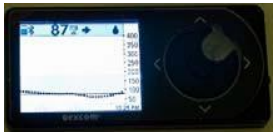
TA2 Challenge: Security at scale

Issues:

- Security across devices with vastly disparate SWaP
- Cost-effective solutions ($2, 5mm^2)
- Requires decentralized operation, ease of use
- Must support authentication, remote attestation, group membership, etc.

[Source: David Culler, UC Berkeley]

1. Patient data download to infected medical office PC via USB results in malware upload



[Source: Jonathan Smith, DARPA]

2.Malware infects more (possibly trusted) devices

[Source: Jonathan Smith, DARPA]

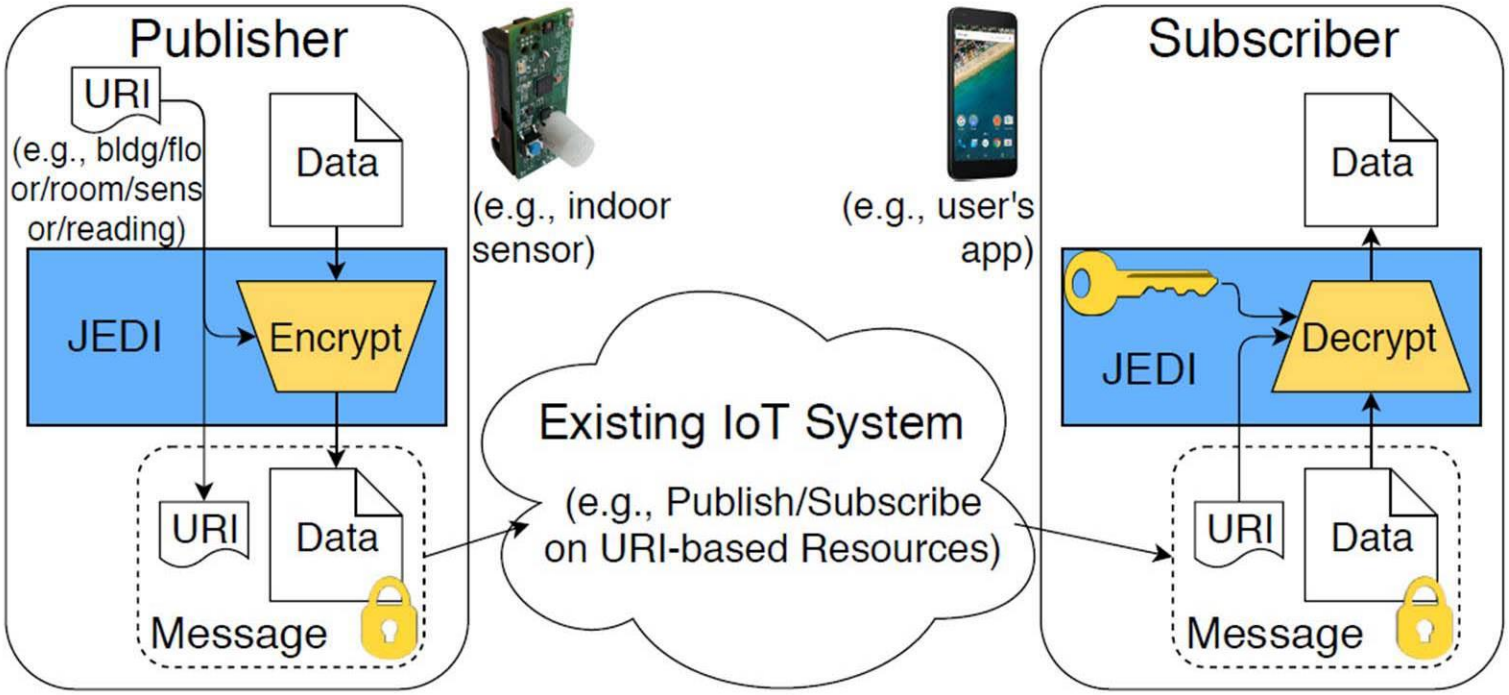
3. Resulting in the Mother of all Botnets

[Source: Fortinet.com]

Technical Area 2 – Many-scale 5G node and network security

Goal: Cost-effective SWaP-conscious crypto, scalable security protocols

Possible Approach: Extend Berkeley JEDI

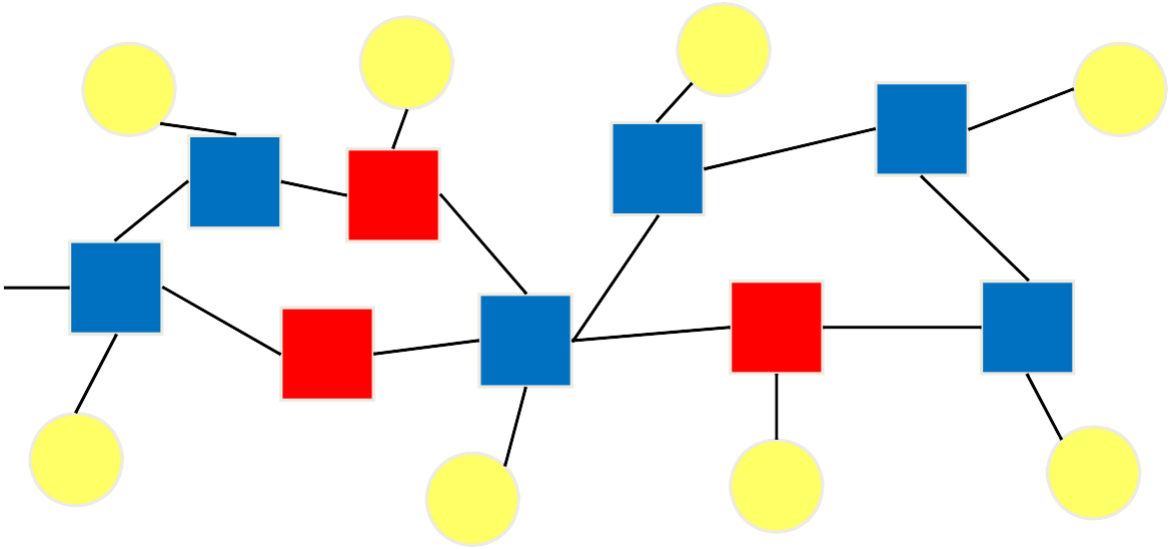


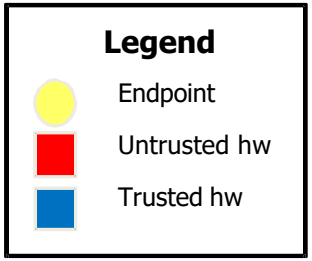
[Source: David Culler, UC Berkeley]

TA3 Challenge: Operating over Untrusted Nodes and Nets

Network slices:

Virtual networks with configurable performance characteristics operating over shared hardware





Issues:

- Sharing of hardware/resources create potential timing channels
- Threats from untrusted network elements: Who owns that net?

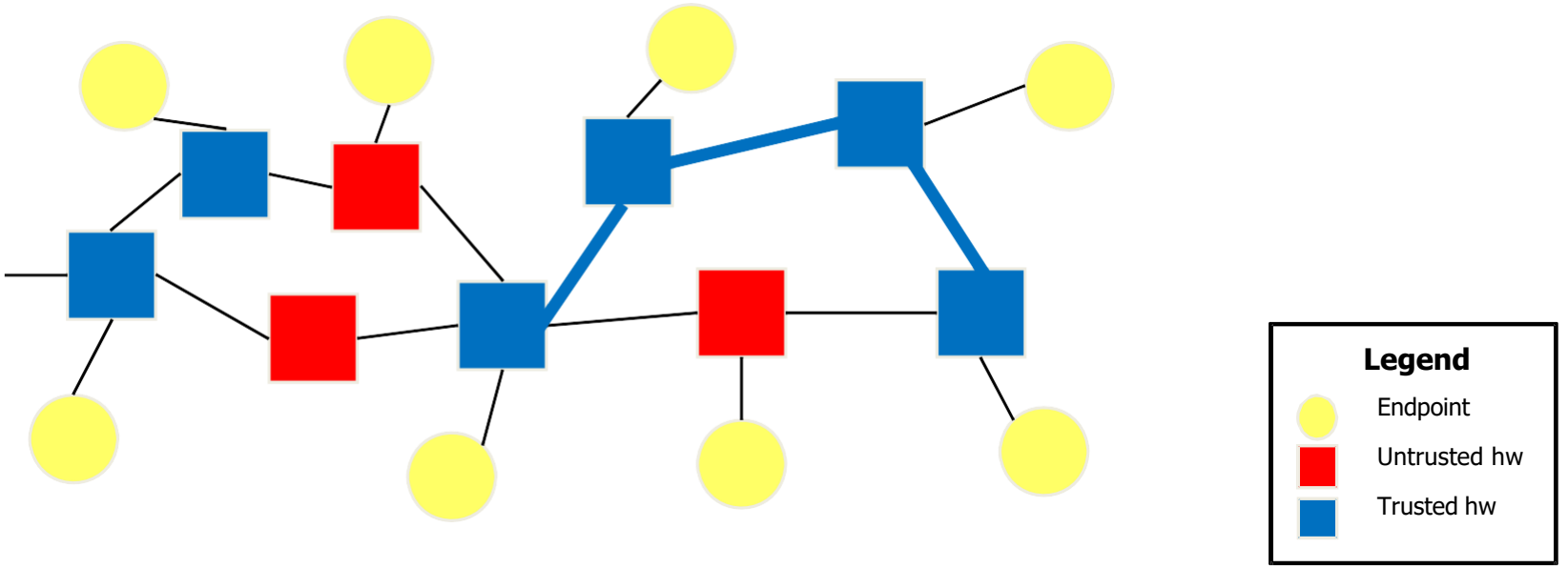
Technical Area 3 – Secure Slices

Goal: Provide security over network resources provided by and shared with unknown entities

Approaches: Route selection avoids:

(1) Nodes that can't attest

(2) Shared resources

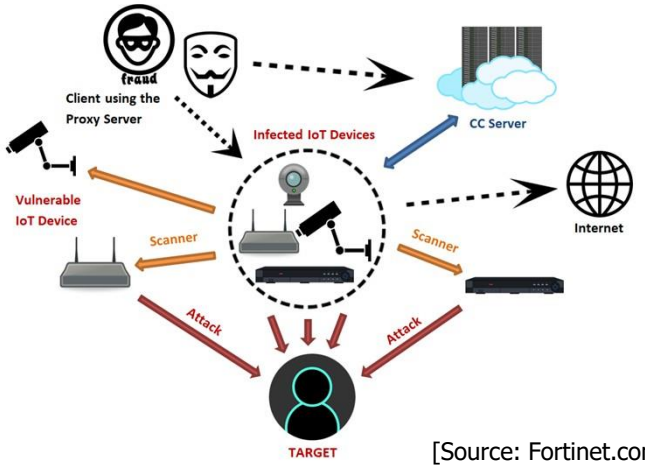


TA4 Challenge: Adaptive Adversaries at Tera-node Scale

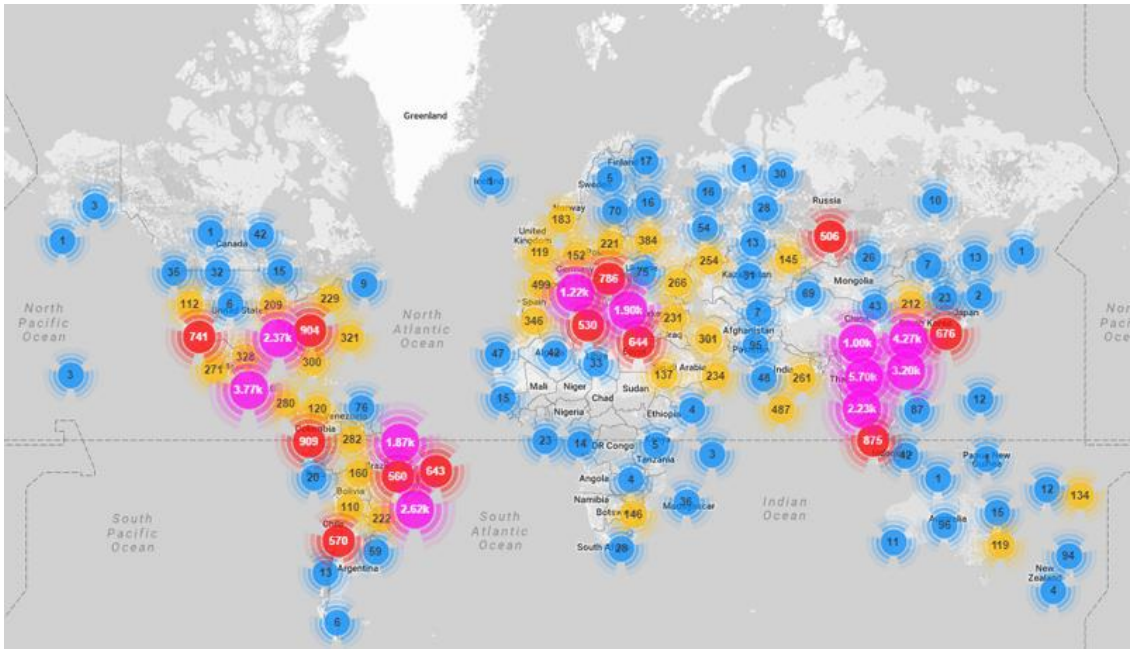
Issue:

- 5G programmability radically increases risk of network attack

Exemplar: IoT DDoS (Mirai)



[Source: Fortinet.com]



Worldwide Mirai Botnet Infections [Source: Securityledger.com]

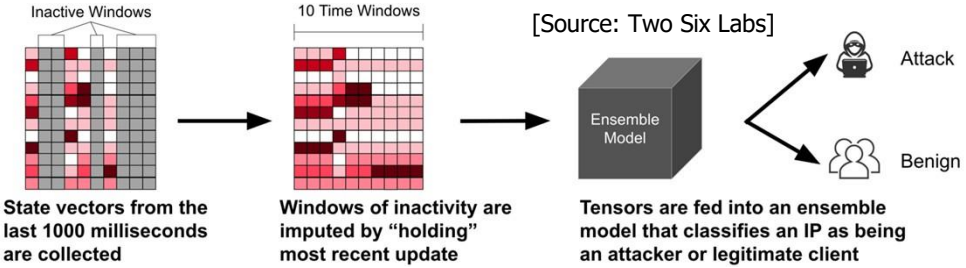
Peak Size: ~600K nodes (cameras, routers, game boxes)
Peak volume: 623 Gbps against Krebs [Antonakakis17]
5G will have 60-600 billion (!) nodes by 2023!!

Technical Area 4 – Principled Programmable Defenses

Goal: Increase security against DDoS attacks

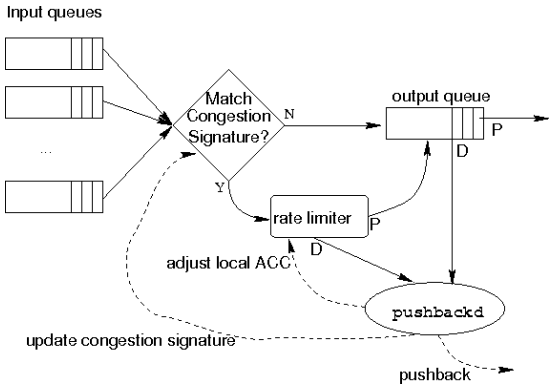
Approach: Use programmable elements of 5G for defense

- Example: Botnet early warning using machine learning (XD3: Two Six Labs)



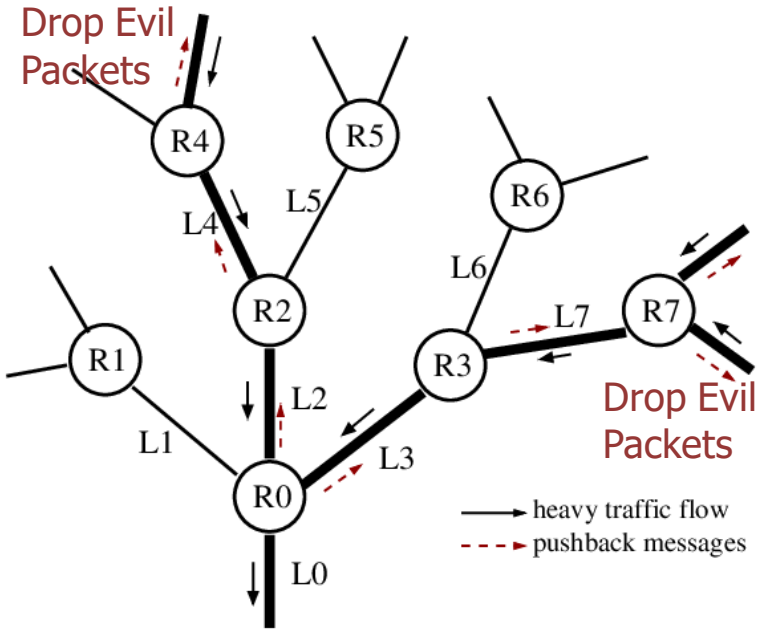
[Source: Two Six Labs]

- Warning triggers deployment of Ioannidis and Bellovin "Pushback"



[Source: Steven Bellovin, Columbia Univ]

On-the-fly node programmability enables real-time distributed detection and diagnosis of attacks and deployment of appropriate defenses



[Source: Steven Bellovin, Columbia Univ]

Notional OPS-5G Technical Area and Program Metrics

	Phase 1 (18 months)	Phase 2 (18 months)	Phase 3 (12 months)
TA1 Precision, recall	60%, Independent Test & Evaluation (ITE)-chosen document	80%, ITE-chosen content and doc	95%, ITE-chosen content and doc
TA2 Security/SWaP	256-bit "encrypt & sign" in < 10 sec using < 70% battery	Resist ITE penetration test of many-to-many IoT for 4 hrs using < 50% battery	Resist ITE penetration test on 10K IoT+User Equipment for 2 days using < 25% battery
TA3 Reduction in secure slice timing channel capacity	3x	10x	50x
TA4 Mirai mitigation time	60 sec on 1G emulated nodes	1 sec on 10,000 IoT nodes	60 sec on 1T emulated nodes
Milestone Demonstrations	Secure voice call between DARPA and USR&E test-site	Data from 1K devices to DARPA over untrusted hardware	Commercial availability in User Equipment and at least 1 US mobile network operator

Independent Test and Evaluation (ITE)

- Voice of the Offense (for Performers)
- Evaluation and Assessment (for DARPA)
- Will use USG entity, e.g., NSA, LTS, Sandia

OPS-5G Summits and 5G Standards

- Transition requires adoption of OPS-5G designs into formal 5G standards
- Program will continually engage with 5G standards committees and US carriers at "summits"

www.darpa.mil